McDonald Hopkins

A business advisory and advocacy law firm®

August 4, 2023

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Loren D. Stark, Co. – Incident Notification

Dear Attorney General Formella:

McDonald Hopkins PLC represents Loren D. Stark Co. ("LDS"). I am writing to provide notification of an incident at LDS that may affect the security of personal information of fifty eight (58) New Hampshire residents. LDS is reporting this incident on behalf of its affected business partners whom LDS maintained data for. By providing this notice, LDS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On November 5, 2023, LDS detected unauthorized access to certain systems on its network as a result of a cybersecurity incident. Upon detecting the incident, LDS immediately worked to remediate the issue and commenced a prompt and thorough investigation. As part of our investigation, LDS worked very closely with third party cybersecurity professionals experienced in handling these types of incidents. After a thorough and detailed forensic investigation and comprehensive manual document review of the files potentially involved in the incident, on June 16, 2023, LDS determined that individual personal information was present on files that could have been accessed or acquired by an unauthorized party. LDS immediately notified affected business partners about the incident, and offered to notify affected individuals on their behalf. LDS verified individual address information from affected business partners on July 28, 2023. The information involved includes individual

LDS has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, LDS wanted to inform you (and the affected business partners and residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. LDS is providing the affected residents with written notification of this incident commencing on or about August 4, 2023 in substantially the same form as the letter attached hereto. LDS is also offering the affected residents complimentary membership with a credit monitoring service. LDS

will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. LDS will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At LDS, protecting the privacy of personal information is a top priority. LDS is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. LDS continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at or

Very truly yours,

Nicholas A. Kurk

Encl.

LDSCO
Loren D. Stark Company

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<VAR DATA 3 – VARIABLE HEADER>>

Dear <<Name 1>>:

We are writing with important information regarding a data security incident that affected our organization. Loren D. Stark Company ("LDS") is a retirement plan consulting firm that provides certain retirement planning services for <<Var Data 2 – Data Owner Name>>. The privacy and security of the personal information we maintain is of the utmost importance to LDS. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

LDS detected unauthorized access to certain systems within its network environment as a result of a cybersecurity incident. The incident resulted in the potential unauthorized access and/or acquisition of certain files from portions of the network on October 18, 2022.

What We Are Doing

Upon detecting the incident, LDS secured the network environment and commenced a prompt and thorough investigation in consultation with third-party cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of the unauthorized activity, and what if any individual personal information may have been accessed or acquired by an unauthorized party. After a thorough and detailed forensic investigation and comprehensive manual document review of the files potentially involved in the incident, on June 16, 2023, LDS determined that your personal information was present on files that could have been accessed or acquired by an unauthorized party.

What Information Was Involved

The data potentially involved included your .

What You Can Do

To date, we have no evidence that any of your information has been misused, however, we wanted to notify you about this incident out of an abundance of caution. To protect you from the potential misuse of your information, we are providing you access to credit monitoring and identity protection services through Equifax Credit Watch Gold.

This letter also provides other precautionary measures you can take to protect your information from potential misuse, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports on a regular basis for fraudulent or irregular activity.

Please accept our apology that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of the personal information in our possession, and have taken steps to further protect unauthorized access to individual records.

For More Information

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at . This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, from 8:00 a.m. to 8:00 p.m., Central Time, excluding holidays.

Sincerely,

Loren D. Stark Company

OTHER IMPORTANT INFORMATION

1. **Enrolling in Complimentary** **Month Credit Monitoring.**
   Enter your Activation Code:
   Enrollment Deadline:

Equifax Credit Watch™ Gold
*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features
- Credit monitoring with email notifications of key changes to your Equifax credit report.
- Daily access to your Equifax credit report.
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites.
- Automatic fraud alerts[2], which encourage potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock.[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf.
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.[4]

Enrollment Instructions
Go to
Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.